INTERNATIONAL MARITIME ORGANIZATION

IMO

E

MARITIME SAFETY COMMITTEE
78th session
Agenda item 7

MSC 78/WP.13
19 May 2004
Original: ENGLISH

MEASURES TO ENHANCE MARITIME SECURITY

Report of the Working Group on Maritime Security

1 General

1.1 The Working Group on Maritime Security (MSWG) met from 13 to 19 of May 2004 under the Chairmanship of Mr. F. Wall (United Kingdom).

1.2 The Group was attended by delegations from the following Member Governments:

ANTIGUA AND BARBUDA
ALGERIA
ARGENTINA
AUSTRALIA
BAHAMAS
BAHRAIN
BARBADOS
BELGIUM
BRAZIL
BULGARIA
CANADA
CHILE
CHINA
CYPRUS
DOMINICA
FINLAND
FRANCE
GERMANY
GHANA
GREECE
ICELAND
INDIA
INDONESIA
IRAN (ISLAMIC REPUBLIC OF)
IRELAND
ITALY
JAMAICA
JAPAN
KENYA
KUWAIT
LATVIA
LIBERIA
LITHUANIA
MALAYSIA
MALTA
MARSHALL ISLANDS
MEXICO
NETHERLANDS
NEW ZEALAND
NIGERIA
NORWAY
PANAMA
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF KOREA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SIERRA LEONE
SINGAPORE
SOUTH AFRICA
SPAIN
SWEDEN
THAILAND
TURKEY
UKRAINE
URUGUAY
UNITED KINGDOM
UNITED REPUBLIC OF TANZANIA
UNITED STATES
VENEZUELA
YEMEN

and the following Associate Member of IMO:

HONG KONG, CHINA

1.3 The session was also attended by representatives from the following United Nations specialized agency:

INTERNATIONAL LABOUR ORGANIZATION (ILO)

1.4 The session was also attended by observers from the following intergovernmental organizations:

EUROPEAN COMMISSION (EC)
INTERNATIONAL MOBILE SATELLITE ORGANIZATION (IMSO)
PORT MANAGEMENT ASSOCIATION OF WEST AND CENTRAL AFRICA (PMAWCA)

and by observers from the following non-governmental organizations in consultative status:

INTERNATIONAL CHAMBER OF SHIPPING (ICS)
INTERNATIONAL CHAMBER OF COMMERCE (ICC)
INTERNATIONAL CONFEDERATION OF FREE TRADE UNIONS (ICFTU)
THE INTERNATIONAL MARINE CONTRACTORS ASSOCIATION (IMCA)
INTERNATIONAL MARITIME PILOTS' ASSOCIATION (IMPA)
INTERNATIONAL RADIO-MARITIME COMMITTEE (CIRM)
THE BALTIC AND INTERNATIONAL MARITIME COUNCIL (BIMCO)
INTERNATIONAL ASSOCIATION OF CLASSIFICATION SOCIETIES (IACS)
OIL COMPANIES INTERNATIONAL MARINE FORUM (OCIMF)
INTERNATIONAL FEDERATION OF SHIPMASTERS' ASSOCIATIONS (IFSMA)
INTERNATIONAL ASSOCIATION OF INDEPENDENT TANKER OWNERS (INTERTANKO)
INTERNATIONAL COUNCIL OF CRUISE LINES (ICCL)
INTERNATIONAL PARCEL TANKERS ASSOCIATION (IPTA)
INTERNATIONAL ASSOCIATION OF MARINE AIDS TO NAVIGATION AND LIGHTHOUSE AUTHORITIES (IALA)
WORLD NUCLEAR TRANSPORT INSTITUTE (WNTI)
THE ASSOCIATION OF EUROPEAN SHIPBUILDERS AND SHIPREPAIRERS (AWES)
FRIENDS OF THE EARTH INTERNATIONAL (FOEI)
INTERNATIONAL ASSOCIATION OF PORTS AND HARBORS (IAPH)

Terms of reference for the Working Group

2 The working group, taking into account the relevant outcome of the sub-committees concerned and the decisions taken and comments made in plenary, was required to:

.1 consider and advise the Committee on:

.1 the wording of SOLAS regulation XI-1/5.5.2 with a view to incorporating the practice recommended in resolution A.911(22) regarding uniform wording in referencing to IMO instruments (operative paragraph 4(a) of

resolution A.959(23) on Format and Guidelines for the Maintenance of the Continuous Synopsis Record (CSR));

.2 the issue raised by DSC 8 with respect to the cargo-related IMO instruments identified by DSC 8 which may need to be amended so as to include appropriate security related provisions (paragraph 2.11 of document MSC 78/13);

.3 the views of COMSAR 8 on long range identification and tracking (LRIT) as set out in paragraphs 22.2.1 to 22.2.5, 22.2.7, 22.2.8, 22.2.10 and Annex of MSC 78/7 as amended by MSC 78/7/Corr.1;

.4 the views of COMSAR 8, taking into account document MSC 78/7/8, with respect to the following aspects of LRIT:

.1 that, from the security point of view, the only information which needs to be provided by a ship is the identity of the ship, its location (latitude and longitude) and the time and date of the position (paragraph 22.2.6 of MSC 78/7, as amended by MSC 78/7/Corr.1); and

.2 that it should not be interfaced with AIS (paragraph 22.2.9 of MSC 78/7, as amended by MSC 78/7/Corr.1);

.5 the issue of the provision of LRIT information to a coastal State by ships exercising the right of innocent passage and not intending to proceed to a port facility under the jurisdiction of a coastal State (paragraph 23 of MSC 78/7, as amended by MSC 78/7/Corr.1);

.6 the role of the Organization in collecting, storing and disseminating LRIT information (paragraph 23 of MSC 78/7, as amended by MSC 78/7/Corr.1);

.7 the elements to be included in the impact assessment on LRIT, bearing in mind operative paragraph 2 of Conference resolution 3 of the 2002 SOLAS Conference;

.8 the proposal of the United States (MSC 78/3/5) relating to adoption of a new regulation XI-2/14 on LRIT in the light of the work done by COMSAR 8 on the issue of LRIT and in view of the discussions in plenary up to the establishment of the MSWG;

.9 the proposal regarding the actions in relation to “distress/security double alerts” (paragraphs 2 to 3 of MSC 78/7/3) with a view of establishing the preliminary advice that can be offered in this respect at this stage;

.10 the proposal regarding the adoption of an MSC Circular aiming at providing assistance, to governmental organizations on matters related to regulation XI-2/6 and XI-2/7 (MSC 78/7/7 and MSC 78/7/7/Corr.1) bearing in mind he fact that a number of Contracting Governments may have already put in place corresponding arrangements;

.11 the proposal (MSC 78/7/5) regarding the guidance which the Committee may issue in the form of an MSC Circular on the security measures and procedures to be applied during ship/port interface when either the ship or the port facility do not comply with the requirements of chapter XI-2 and of the ISPS Code;

.12 the proposal (paragraph 3.3 of MSC 78/7/6) regarding the establishment of a mechanism for resolving conflicting interpretations of the ISPS Code;

.13 the proposal regarding the guidance which the Committee may issue in the form of an MSC Circular on the issue of shipyards;

.14 the proposal regarding the guidance which the Committee may issue in the form of an MSC Circular on the security measures and procedures to be applied by a ship, which is required to comply with the requirements of chapter XI-2 and of the ISPS Code, when it interfaces with an FPSO or an FSU; and

.15 the request to provide guidance on the interpretation of the provisions of the ISPS Code relating to the ability of seafarers to go ashore for shore leave and for joining and leaving a ship after the agreed period of service; and

.2 finalize the proposed guidelines on Control and Compliance Measures to Enhance Maritime Security (Annex to document MSC 78/7/Add.1), taking into account documents MSC 78/7/9, MSC 78/7/11, MSC 78/7/12, MSC 78/7/13, MSC 78/7/14 and MSC 78/7/15; and to submit them to the Committee for consideration and adoption;

.3 prepare and submit to the Committee for consideration and adoption an MSC Circular outlining the decision of the Committee to consider the proposals (MSC 78/7/3) in relation to "false security alerts" and "distress/security double alerts" further at its next session in the light of the experience to be gained and inviting interested parties to submit information and data in relation to actual cases they might experience during the period between 1 July 2004 and 15 October 2004. In this respect the MSWG should advise the Committee whether the information and data to be submitted needs to identify the particular ships involved in the specific incidents to be reported; and

.4 submit its report for the consideration of the Committee not later than Thursday, 20 May 2004.

CONTINUOUS SYNOPSIS RECORD (CSR)

3 The Group concluded that the Continuous Synopsis Record (CSR) is now a statutory document, which is required to be carried by every ship to which chapter I applies and which is subject to port State control inspections under the provisions of SOLAS regulation I/19. As such, its format needs to be standardized and it should be treated in the same manner as the certificates and documents a ship is required to carry under the provisions of SOLAS chapter I or under the provisions of the codes which have been made mandatory under SOLAS 74. The Group noted that, unlike the various certificates and documents a ship is required to carry and which are

issued anew each time a ship is transferred to the flag of another Contracting Government, the CSR remains with the ship throughout its life, but is added to each time a ship changes flag.

4 The Group concluded that, before making the format and the guidelines for the maintenance of the CSR mandatory under the provisions of SOLAS chapter XI-1/5, it will be necessary to allow a reasonable period for Contracting Governments to gain practical experience through the use of the format and the guidelines for the maintenance of the CSR as detailed in resolution A.959(23). This will enable, if necessary, the improvement of the format and the guidelines for the maintenance of the CSR. The Group noted that, although a practice relating to the issue of other certificates and documents has evolved over the years and is followed by all Contracting Governments, the CSR is a new document and thus guidelines for the issue and maintenance of the CSR need to evolve in order to develop a standard practice for its use.

5 The Group recalled that FSI 12 recommended the adoption of a number of amendments to the provisions of SOLAS regulation XI-1/5 and to the provisions of resolution A.959(23) so as to include the proposed unique Company and registered owner identity numbers. However, the Group noted that the amendments proposed by FSI 12 do not foresee a unique identity number for bareboat charterers and, since on certain occasions an Administration may issue CSRs as a result of a ship flying its flag under the terms of the registration of a bareboat charter, this aspect needs to be addressed. The Group agreed that in order to avoid repeated amendments of regulation XI-1/5 and of the format and the guidelines for the maintenance of the CSR it will be necessary to adopt the relevant amendments at the same time; to provide a reasonable period for a phased-in implementation of the mandatory requirements; and to clarify whether it will be necessary to include the unique identity numbers in CSRs issued prior to the entry into force of the contemplated amendments which may be valid at the particular time.

6 The Group agreed to recommend that, although there is a need to make the format and the guidelines for the maintenance of the CSR as detailed in resolution A.959(23) mandatory under the provisions of regulation XI-1/5, it would not be advisable to proceed with any amendments of the provisions of regulation XI-1/5 at this stage.

7 The Group also agreed to suggest that the Committee should urge Contracting Governments to adhere to the guidance given in resolution A.959(23) until the format and the guidelines for the maintenance of the CSR are made mandatory under the provisions of regulation XI-1/5.

REVIEW OF CARGO-RELATED IMO INSTRUMENTS

8 The Group noted that paragraph 9.8 of document DSC 8/15 and the report of the drafting group (document DSC8/WP.4) identified a number of cargo-related IMO instruments (the ISPS Code; the CSC Convention; Part B of the STCW Code; the INF Code; the BC Code; the IBC Code; the IGC Code; the IMO Model course 1.10; and the FAL Convention) which may need to be amended so as to include appropriate security related provisions. However the DSC drafting group did not expand on the need to undertake the proposed task or on how the instruments cited are "deficient" in terms of security.

9 As a result, the Group agreed to suggest that, at this stage, the issue raised by DSC 8 should not be pursued further and that the DSC Sub-Committee should be instructed to revisit the issue in accordance with paragraph 12 below.

10 The Group was of the view that the Committee needs to discuss, first, the necessity and the desirability of embarking on the review and amendment of the cargo-related instruments

referred to above. Embarking on a review and amendment of the ISPS Code at this stage may be premature and may, in fact, create "wrong" impressions. Whilst the industry is struggling to implement the special measures to enhance maritime security, an announcement that the Organization is embarking on amendments to existing instruments may prove discouraging and counter-productive and, bearing in mind that access control is one of the fundamental functional requirements of the ISPS Code, may even imply that the ISPS Code is not adequate.

11 The Group concluded that for the Committee to fulfil its mandate under operative paragraph 1 of resolution A.924(22), which directs the Committee to review "*any other relevant IMO instrument under their scope and/or to adopt other security measures and, in the light of such a review, to take prompt action as appropriate*", the Committee needs to have before it an overall picture of the actions required. This will enable the Committee to engage in any policy and planning discussions on the matter an integrated and comprehensive manner.

12 For this purpose the Group agreed to recommend that the Committee should instruct the various Sub-Committees, under their existing work programme and agenda on Maritime Security, to identify the various instruments under their responsibility, which may need to be reviewed and amended so as to include appropriate security-related provisions. In this respect the Sub-Committees should bear in mind the functional requirements of the ISPS Code and in particular those relating to access control and handling of cargo. The Sub-Committees should be instructed to expand on the need to amend each of the instruments which they will be identifying; to prioritize the work they will be suggesting and to indicate, bearing in mind their other work load and priorities, the time (number of sessions) needed to amend each of the instruments.

LONG RANGE IDENTIFICATION AND TRACKING

Outcome of COMSAR 8

13 The Group considered the outcome of COMSAR 8 in relation to long-range identification and tracking (LRIT) as set out in paragraphs 22.2.1 to 22.2.5, 22.2.7, 22.2.8, 22.2.10 and annex of document MSC 78/7 as amended by MSC 78/7/Corr.1.

14 The Group agreed to recommend that the Committee should reaffirm the endorsement the view of COMSAR 8 referred to in paragraph 13 above, subject to the conclusions and recommendations of the Group in relation to the role of the Organization in collecting, storing and disseminating LRIT information (paragraph 30 below).

LRIT parameters to be reported

15 The Group agreed that, from the security point of view, the only information which needs to be provided by a ship is the identity of the ship, its location (latitude and longitude) and the time and date of the position. No other information is needed.

16 The Group agreed that the LRIT system should be designed to ensure the integrity of the data and to prevent the intentional transmission of false information.

17 The Group agreed that the provision of any other information will increase the total cost, may lead to an overflow of information and will not contribute to the enhancement of security. Furthermore, the Group noted that some of the information proposed by the Netherlands and Sweden (document MSC 78/7/8) for inclusion and transmission would require manual input from the ship, which would afford undesirable opportunities for the provision of false or misleading information.

18 The Group noted that the flag State has the right, at any time, to request and require ships entitled to fly its flag to provide whatever information, including LRIT information, that State considers necessary. Likewise, from the moment a ship has advised a port State of its intention to enter a port facility located within its territory, the port State may invoke the provisions of regulation XI-2/9 and request the ship to provide further information which may include LRIT. The Group also noted that, although the rights of a coastal State are rather limited with regard to LRIT, nothing prohibits a coastal State from approaching the flag State of a particular ship with a request, in the light of any security related concerns the coastal State may have, for additional information.

19 The Group agreed to recommend that the Committee should endorse the view of COMSAR 8 in this respect, namely that, from the security point of view, the only information which needs to be provided by a ship is the identity of the ship, its location (latitude and longitude) and the time and date of the position (paragraph 22.2.6 of document MSC 78/7, as amended by MSC 78/7/Corr.1).

Interface of LRIT with AIS

20 The Group agreed that LRIT should not be interfaced with AIS since some of the AIS messages, under the existing AIS performance standards, are input manually and may lead to transmission of inaccurate or intentionally misleading information. In addition, the Group was of the view that further consideration of the interface of LRIT with AIS would lead to the addition of another level of complexity in the consideration of the issue.

21 The Group agreed to recommend that the Committee should endorse the view of COMSAR 8 in this respect, namely that LRIT should not be interfaced with AIS (paragraph 22.2.9 of document MSC 78/7, as amended by MSC 78/7/Corr.1).

Provision of LRIT information to a coastal State

22 The Group discussed extensively the issue of the provision of LRIT information to a coastal State by ships exercising the right of innocent passage and not intending to proceed to a port facility under the jurisdiction of that coastal State. However, the Group was unable to conclude on the matter.

23 The Group agreed that coastal States should be able to receive LRIT information from ships exercising the right of innocent passage and not intending to proceed to a port facility under their jurisdiction.

24 The delegation of the United States expressed the view that one of the fundamental purposes of LRIT was to permit Coastal States to have sufficient time to evaluate the security risk posed by a ship off its coast and to respond if necessary, to reduce that risk. Therefore, the distance off the coast must be set at a level that achieves this purpose. For this reason, the United States expressed serious concern with the proposal of some States to set the distance at 200 nautical miles as being contrary to the security benefit to be provided by LRIT to coastal States. The United States also stated that 200 nautical miles appeared to be an arbitrary distance, only offered because it corresponded with the extent of the EEZ under UNCLOS. Since the LRIT amendment is being developed in the security context, and UNCLOS generally does not permit Coastal States to exercise security jurisdiction over transiting ships in the EEZ, the overlap of the LRIT distance with the EEZ would create substantial confusion and complications

under UNCLOS. The United States therefore reiterated its view that the distance off the coast of a Coastal State should be allowed up to 2,000 nautical miles.

25 A number of delegations expressed the view that the distance off the coast of the coastal State should be limited and suggested various figures ranging up to 200 nautical miles off shore. However, a number of delegations observed that, bearing in mind the speed of a ship, a reduced range may not afford a coastal State a reasonable opportunity or period of time to assess the security threat a particular ship may present and put in place appropriate protective measures.

26 A number of delegations expressed the view that, instead of a distance off shore, the period of time a ship may require to reach the coast of a coastal State should be used as a criterion. However, a number of delegations indicated that the speed of a ship may be varied as a result of prevailing weather or other reasons and thus, this may not achieve the objective of providing to a coastal State LRIT information.

27 The Chairman suggested that in view of the fact that the Group had agreed that coastal States should be able to receive LRIT information, this may be done on a world-wide basis and left to the discretion of each Contracting Government, as a coastal State, to determine the distance off shore or the period of time, based on its own security needs. However, in this context, Administrations should retain the right to curtail the distance off shore or the time based on their own security considerations. Contracting Governments shall specify, and shall communicate to the Organization, either the distance from their coast or the period of time a ship may require to reach their coast, during which they require the provision of identification and tracking information. The Organization shall circulate the communications received for the information of all Contracting Governments.

28 The Group was advised that, from the technical point of view, since the system was designed to enable Administrations to receive LRIT information for all ships entitled to fly its flag, irrespective where such ships may be located, the provision of LRIT to a coastal State is matter of programming appropriate software filters which could be done once a decision has been made. This aspect is a matter that may also be addressed in the context of the recognition and approval of the LRIT providers. In addition, even if the Committee were unable to reach a definite decision on the issue at this stage, this need not adversely affect the work of the COMSAR Sub-Committee in relation to the development of LRIT.

29 The Group agreed to advise the Committee that Contracting Governments are not yet ready to reach an agreement on this issue and that the COMSAR Sub-Committee should be instructed to develop the system in such a way that it envisages three classes of users, each one of them entitled to receive different LRIT information. With respect to port States and coastal States the criterion to be used may either be a distance off the coast of a Contracting Government or the period of time a ship may require to reach the coast of a Contracting Government.

30 The Group agreed to recommend that the Committee should instruct the COMSAR Sub-Committee to ensure that the LRIT system:

.1 is capable of being switched off on board in cases where the Administration considers that the receipt of information by another Contracting Government may compromise the safety or security of the ship or of the Administration; and

.2 is capable of preventing a named coastal State from receiving LRIT information, where requested by the Administration, if the coastal State as a Contracting Government is otherwise entitled to receive that information.

The role of the Organization

31 The Group considered that if the Organization were to assume any role in relation to LRIT, there would be a need to develop and agree a legal, administrative and financial framework for its involvement which will add another layer of complexity and may even require the approval of the Council and of the Assembly. The Group therefore agreed to recommend that the Organization should not be involved in collecting, storing and disseminating LRIT information.

32 The Group also agreed to recommend that the Committee should approve the LRIT providers and that Contracting Governments should be able to purchase LRIT information directly from the approved LRIT providers, subject to the provisions in paragraphs 28 and 29 above.

33 In lieu of the role of the Organization in collecting, storing and disseminating LRIT information, the Group agreed to recommend that the Committee should instruct the COMSAR Sub-Committee to develop and propose conditions which the Committee may impose on a LRIT provider when considering its approval. In addition, the Group recommended that the COMSAR Sub-Committee be instructed to develop and propose a robust intergovernmental oversight scheme for the approved LRIT providers through which the adherence of the LRIT providers to the conditions imposed on them, at the stage of their approval, can be verified in a transparent manner to the satisfaction of all Contracting Governments.

Impact study

34 The Group recalled that COMSAR 8 advised the Committee that considerable work needs to be done before the COMSAR Sub-Committee will be in a position to advise the Committee on the issue of LRIT. In addition the Group also recalled that COMSAR 8 had indicated if LRIT service providers, other than Inmarsat, were to be allowed to provide LRIT services, it would be necessary, *inter alia,* to develop and agree:

.1 the functional requirements which LRIT systems have to meet;
.2 the criteria for assessment of such systems;
.3 the security requirements to be complied with by such systems;
.4 the procedures for recognition and acceptance of such systems; and
.5 the oversight of such LRIT service providers.

35 The Group concluded that the material available so far, on which an impact assessment may be based, is very limited and thus the possible outcomes of any impact assessment on LRIT may be diverse and misleading and may even be disputed.

36 However, the Group agreed to recommend that, in the light of the conclusions of the Group in relation to the outcomes of COMSAR 8 relating to LRIT and on the role of the Organization in collecting, storing and disseminating LRIT information, the conduct of an impact study, as suggested in operative paragraph 2 of Conference resolution 3 of the 2002 SOLAS Conference, appears, at this stage, not to be desirable.

37 The Group however, agreed that if, in addition to security, the purpose of LRIT is to be expanded to include safety and pollution prevention aspects, or if the architecture of the LRIT envisaged by COMSAR 8 is to be amended (for example in such a way to require the installation

on board of dedicated equipment), then the issue of the impact study might need to be reconsidered.

The proposal of the United States (document MSC 78/3/5)

38 The delegation of the United States advised the Group that document MSC 78/3/5 was submitted to MSC 78 prior to COMSAR 8. The Working Group decided, in the light of the discussions on LRIT at COMSAR 8 and in plenary, and since the draft regulation relating to LRIT was included in the COMSAR 8 report (documents COMSAR 8/18, COMSAR 8/WP.5 and MSC 78/7) and would be further discussed at COMSAR 9, discussion of the United States paper was premature.

Other technical aspects

39 The Group agreed to recommend that the Committee should instruct the COMSAR Sub-Committee to consider and address the priority of the LRIT signal.

40 Whilst discussing the issue of the priority of the LRIT signal the Group noted that the current performance standards for ship security alert systems do not envisage any priority for the ship security alert signal and thus it recommends that Committee should also instruct the COMSAR Sub-Committee to consider and address this issue.

41 The Group noted that a number of delegations were putting forward proposals to expand the scope of the LRIT from being a security tool to a tool which may be used for safety and pollution prevention. Thus, the Group recommends that the Committee should consider the matter and should define, before COMSAR 9, the purpose and scope of LRIT, so as to enable COMSAR 9 to proceed with its assigned work.

DISTRESS/SECURITY DOUBLE ALERTS

42 The Group agreed to recommend to the Committee for consideration and adoption the guidance in relation to "distress/security double alerts" in the draft MSC Circular set out in annex 1.

MATTERS RELATED TO REGULATION XI-2/6 AND XI-2/7

43 The Group considered the proposal regarding the adoption of an MSC Circular on the receipt and distribution of security alerts and matters related to SOLAS regulations XI-2/6 and XI-2/7 (documents MSC 78/7/7 and MSC 78/7/7/Corr.1).

44 The Group agreed that, bearing in mind the fact that a number of Contracting Governments may have already put in place arrangements addressing the issues raised in documents MSC 78/7/7 and MSC 78/7/7/Corr.1, it was inappropriate, at this stage, to develop such guidance.

45 However, as a result of the discussion of the issue, the Group agreed to recommend to the Committee for consideration and adoption the guidance set out in set out in annex 2.

SECURITY MEASURES AND PROCEDURES TO BE APPLIED DURING SHIP/PORT INTERFACE WHEN EITHER THE SHIP OR THE PORT FACILITY DO NOT COMPLY WITH THE REQUIREMENTS OF CHAPTER XI-2 AND OF THE ISPS CODE

46 The Group agreed to recommend to the Committee for consideration and adoption the guidance set out in paragraphs 2 to11 of the annex to annex 3.

MECHANISM FOR RESOLVING CONFLICTING INTERPRETATIONS OF THE ISPS CODE

[more to come]

SHIPYARDS

47 The Group agreed to recommend to the Committee for consideration and adoption the guidance set out in paragraphs 12 to 17 of the annex to annex 3.

48 The observer from AWES raised concerns as to wide variety of views expressed by national delegations concerning the application of the ISPS Code to shipyards. In application, this lack of unanimity could lead to inequitable implementation of the provisions world-wide, resulting in market distortions in shipbuilding, repair and conversion.

ABILITY OF SEAFARERS TO GO ASHORE FOR SHORE LEAVE AND FOR JOINING AND LEAVING A SHIP

49 The Group agreed to recommend to the Committee for consideration and adoption the MSC Circular set out in annex 4.

GUIDELINES ON CONTROL AND COMPLIANCE MEASURES TO ENHANCE MARITIME SECURITY

[more to come]

Action requested of the Committee

[more to come]

***

ANNEX 1

DRAFT MSC CIRCULAR

False Security Alerts and Distress/Security Double Alerts

1 The Maritime Safety Committee, at its seventy-eighth session (12 to 21 May 2004) exchanged views on a proposal relating to the actions which may be taken in relation to "false security alerts" and "distress/security double alerts".

2 SOLAS regulation XI-2/6 requires ships to be fitted with a ship security alert system (SSAS) which, when activated, shall initiate and transmit a ship-to-shore security alert (security alert) to a competent authority designated by the Administration, indicating that the security of the ship is under threat or it has been compromised. The requirement for the carriage of SSAS, which is a covert system, is additional to the requirement to be provided with radio communication equipment capable of initiating and transmitting distress alerts and piracy attack alarms, both of which are overt systems.

3 Experience of false distress alerts gained since the introduction of GMDSS indicates that a ship may transmit a "false security alert" either as a result of technical failure of the SSAS or due to inadvertent activation of the system. In either case, since SOLAS regulation XI-2/6.2.3 provides that SSAS, when activated, shall not raise any alarm on board the ship, shipboard personnel will be unaware, or unable to establish, whether a security alert is in fact being transmitted.

4 The Committee was therefore requested to advise what action should be taken between the time a security alert is first received ashore and the time that the competent authorities initiate action to address the security alert, bearing in mind that there is a need to determine whether the security alert received ashore is a genuine or a false one.

5 The Committee was also requested to consider what action should be taken in the event of a ship transmitting a distress alert and a security alert (distress/security double alert), either simultaneously or one after the other. In view of the fact that a security incident may lead to a distress situation or a distress situation may be followed by a security incident; and since all ships are capable of transmitting both alerts, simultaneously or in tandem; the competent authorities ashore need to assess the situation so as to determine and prioritise the response to be provided.

6 The Committee, bearing in mind the need to identify the nature and extent of the aspects involved, decided to consider these proposals further at its next session (1 to 10 December 2004) in the light of the actual experience to be gained from the use of ship security alerts systems. In this respect the Committee decided to invite Member Governments and international organizations to submit information and data in relation to actual cases they might experience during the period between 1 July 2004 and 15 October 2004. The Committee also decided that the information and data to be submitted do not necessarily need to identify the particular ships involved in the specific incidents to be reported.

***

ANNEX 2

DRAFT MSC CIRCULAR

MATTERS RELATED TO SOLAS REGULATIONS XI-2/6 AND XI-2/7

Ship Security Alerts

1 The Committee noted that SOLAS regulation XI-2/6.6 requires that an Administration receiving notification of a ship security alert shall notify the States in the vicinity of which the ship is presently operating. The Committee confirmed that the appropriate recipient for such information is the national point of contact as required by SOLAS regulation XI-2/7.2, as notified to, and promulgated by, the Organization in accordance with SOLAS regulation XI-2/13.1.5. Where the State(s) in the vicinity of the ship are non-Contracting parties to SOLAS, such information should be passed via normal diplomatic channels in the most expedient manner.

2 The Committee also noted that although the intended recipient of a security alert was a competent authority designated by the Administration which may be an MRCC, it was possible that covert security alerts could be received by non-designated MRCCs. Guidance on the action to be taken by MRCCs in such instances is detailed in MSC/Circ.1073 on "Directives for maritime rescue co-ordination centres on acts of violence against ships".

Response to Distress/Security Double Alerts

3 The Committee, recognizing the potential consequences of failure to provide a prompt and adequate response to the distress alert element of a "distress/security double alert" situation and, pending further consideration of the issue, recommended that such cases would require an immediate response to the situation arising from the distress alert. However, those responding to the distress alert should be instructed, through the MRCC, to proceed with due care and caution bearing in mind that the security of the ship may have been compromised or be under threat.

***

ANNEX 3

DRAFT MSC CIRCULAR
GUIDANCE RELATING TO THE IMPLEMENTATION OF SOLAS CHAPTER XI-2 AND THE ISPS CODE

1 The Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS), 1974 (London, 9 to 12 December 2002), adopted amendments to the Annex to the Convention, as amended, in particular new chapter XI-2 on Special measures to enhance maritime security; and, the new International Code for the Security of Ships and Port Facilities (ISPS Code).

2 The Maritime Safety Committee, at its seventy-eighth session (12 to 21 May 2004), recognizing and considering the need for additional information to assist Contracting Governments and the industry with the implementation of, and compliance with new SOLAS chapter XI-2 and the ISPS Code, directed its Maritime Security Working Group to examine and provide additional guidance on specific aspects of the measures to enhance maritime security.

3 The guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code, as approved by the Committee, is given at annex.

4 Reference is also made in this context to MSC/Circ.1097 on Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code.

5 Member Governments and international organizations are invited to bring this circular to the attention of national Designated Authorities, Administrations and all parties concerned and responsible for the implementation of maritime security measures.

ANNEX

GUIDANCE RELATING TO THE IMPLEMENTATION OF
SOLAS CHAPTER XI-2 AND THE ISPS CODE

GENERAL

1 The ensuing paragraphs are lifted from the report of the Maritime Security Working Group (MSC 78/WP.[**]) at MSC 78 and are considered to be of valuable guidance for the implementation of SOLAS chapter XI-2 and the ISPS Code on relevant topics.

SECURITY MEASURES AND PROCEDURES TO BE APPLIED DURING SHIP/PORT INTERFACE WHEN EITHER THE SHIP OR THE PORT FACILITY DO NOT COMPLY WITH THE REQUIREMENTS OF SOLAS CHAPTER XI-2 AND OF THE ISPS CODE

Ships

2 The Committee considered the security measures and procedures to be applied during ship/port interface when either the ship or the port facility do not comply with the requirements of chapter XI-2 and of the ISPS Code.

3 The Committee recalled paragraph B/9.51 of the ISPS Code which recommends that the ship security plan (SSP) should establish details of the procedures and security measures the ship should apply when:

.1 it is at a port of a State which is not a Contracting Government;

.2 it is interfacing with a ship to which the ISPS Code does not apply[1];

.3 it is interfacing with a fixed or floating platform or a mobile drilling unit on location; or

.4 it is interfacing with a port or port facility which is not required to comply with chapter XI-2 and part A of the ISPS Code;

and thus considers that guidance, in this respect, is only required for those ships which have not already included appropriate provisions to this end in the approved SSP.

4 The Committee decided to recommend that in such cases, if the ship's approved SSP does not already include provisions as recommended in paragraph B/9.51 of the ISPS Code, the ship should attempt to conclude, if possible, a Declaration of Security or to take the following action:

.1 record the actions taken by the Company Security Officer (CSO) and/or Ship Security Officer (SSO) to establish contact with the Port Facility Security Officer

[1] Refer to further work by the International Maritime Organization pertaining to Enhancement of maritime security and to Establishment of appropriate measures to enhance the security of ships, port facilities, mobile offshore drilling units on location and fixed and floating platforms not covered by chapter XI-2 of the 1974 SOLAS Convention, adopted by the Conference on Maritime Security by resolutions 3 and 7 respectively.

(PFSO), and/or any other persons responsible for the security of the port, ship or platform being interfaced;

.2 record the security measures and procedures put in place by the ship, bearing in mind the security level set by the Administration and any other available security-related information; and complete and sign, on behalf of the ship alone, a Declaration of Security;

.3 implement and maintain the security measures and procedures set out in the Declaration of Security throughout the duration of the interface;

.4 report the actions taken to the CSO and through the CSO to the Administration; and

.5 request the CSO to inform the authorities responsible for the exercise of control and compliance measures (regulation XI-2/9) and the PFSO(s) at the next port(s) of call of the difficulties the ship experienced and of the actions the ship itself took.

5 The Committee recognized that a ship should be able to address most of the ship security activities required by section A/7 of the ISPS Code.

6 In addition the Committee recognized that on certain occasions and, in particular, when a ship is required to call at a port of a State which is not a Contracting Government, the ship may be unable to identify the person responsible for the security of that port or to conclude with such a person a Declaration of Security.

Security concerns

7 The Committee also considered the case where a ship has concerns about the security of a port facility, which is supposed to operate in accordance with an approved Port Facility Security Plan (PFSP).

8 In this respect the Committee decided to draw the attention to the fact that certain of the security measures may be of a covert nature and may not be easily identified. Thus, the Committee recommended that the ship, as a first step, should contact the PFSO and discuss the matter.

9 The Committee recalled the provisions of paragraph B/4.16 of the ISPS Code and recommends that the procedure referred therein should be followed. If no remedial action is agreed between the Contracting Governments concerned, the Committee recommends that the ship, in the absence of any specific provisions to this end in the ship's approved SSP, may either request a Declaration of Security or should follow the steps outlined in paragraph 3.1 to 3.4 above.

Port Facilities

10 The Committee recalled paragraph B/16.56 of the ISPS Code which recommends that the PFSP should establish details of the procedures and security measures the port facility should apply when:

.1 it is interfacing with a ship which has been at a port of a State which is not a Contracting Government;

.2 it is interfacing with a ship to which the ISPS Code does not apply; and

.3 it is interfacing with fixed or floating platforms or mobile offshore drilling units on location;

and thus considers that guidance, is only be required with respect to those port facilities which have not already included appropriate provisions to this end in the approved PFSP.

11 The Committee decided to recommend that as soon as the PFSO becomes aware of the intended arrival of a ship which is required to comply with the requirements of chapter XI-2 and of part A of the ISPS Code, which has been in a port of a non-Contracting Government, or of a ship which is flying the flag of a State which is not a Contracting Government, he/she should contact the authorities responsible for the exercise of control and compliance measure (regulation XI-2/9) and the authorities which approved the PFSP and seek their advice and guidance.

SHIP CONSTRUCTION, CONVERSION AND REPAIR YARDS

12 Ship construction, conversion and repair yards (shipyards) are not specifically referred to in chapter XI-2 or the ISPS Code. However, they may be located adjacent to port facilities and their activities may have an impact on the security of such port facilities or on the security of ships using such port facilities. Shipyards may also interface with ships, which may be required to comply with the ISPS Code.

13 The designation of shipyards as distinct port facilities is a matter to be considered by the Contracting Government (or the Designated Authority) within whose territory the shipyard is located. The designation may depend on local circumstances and the result of the Port Facility Security Assessment (PFSA) of the shipyard itself or of the PFSAs relating to adjacent port facilities. If a shipyard is designated as a port facility a PFSO shall be appointed and the Contracting Government (or the Designated Authority) shall approve the shipyard's PFSP.

14 A ship under construction is not considered to be a ship, in the context of chapter XI-2 and of part A of the ISPS Code, until the relevant statutory certificates have been issued. This includes the preparation of the ship's Ship Security Assessment (SSA), the preparation and approval of the SSP, the verification of the implementation of the ship's security measures and procedures and the issue of the ship's International Ship Security Certificate (ISSC), or alternatively the verification of the requirements leading to the issue of an Interim ISSC.

15 When a ship is under construction, the security of the ship is the responsibility of the shipyard. Once the ship receives its ISSC (or Interim ISSC) the ship will have to comply with the provisions of its [approved] SSP. This may require the CSO and/or the SSO to discuss security measures and procedures with the shipyard, irrespective of whether the shipyard has a PFSO or not. This may lead to an agreement on the respective responsibilities for security measures to protect the ship which in turn may involve the conclusion of a Declaration of Security.

16 The position of ships under conversion or repair will depend on the approach the ship's Administration takes regarding the suspension or revocation of the certificates of the ship, including the ISSC, and, in practice, the extent to which the ship's personnel remains on board

and retains the capability to exercise their duties under the SSP. If the certificates of the ship, including the ISSC, are suspended or revoked, responsibility for the security of the ship would in practice rest with the shipyard and may require the conclusion of an agreement between the owner and the shipyard. If the nature of the repairs means that all, or part, of the shipboard personnel remains on board and the certificates of the ship, including the ISSC, have not been suspended or revoked, the sharing of security responsibilities between the ship and the shipyard will have to be agreed and this may involve the conclusion of a Declaration of Security.

17 The approach taken to the security of ships undertaking sea trials is the responsibility of the State whose flag the ship is flying at the time of its trials. Some form of security assessment should be undertaken in respect of the ship and security measures and procedures put in place for the duration of the trials to the satisfaction of the relevant State.

FPSOs AND FSUs

[more to come]

***

ANNEX 4

DRAFT MSC CIRCULAR
SHORE LEAVE AND ACCESS TO SHIPS UNDER THE ISPS CODE

1 The Conference of Contracting Governments to the International Convention for the Safety of Lives at Sea (SOLAS), 1974 (London, 9 to 12 December 2002), adopted, *inter alia*, amendments to the Annex to the Convention, as amended, in particular new chapter XI-2 on Special measures to enhance maritime security and the new International Code for the Security of Ships and Port Facilities (ISPS Code).

2 The Conference also adopted Conference resolution 11 on Human-element-related aspects and shore leave for seafarers which, *inter alia*, urged Contracting Governments to take the human element, the need to afford special protection to seafarers and the critical importance of shore leave into account when implementing the provisions of SOLAS chapter XI-2 and the ISPS Code.

3 The Maritime Safety Committee, at its seventy-eighth session (12 to 21 May 2004), recognizing and considering the need for additional information to assist Contracting Governments and the industry to comply with the spirit of Conference resolution 7, while at the same time meeting their obligations under SOLAS chapter XI-2 and the ISPS Code, directed its Maritime Security Working Group to examine and provide additional guidance on specific aspects of shore leave and access to ships under the ISPS Code.

4 The guidance relating to shore leave and access to ships, as approved by the Committee, is given at annex.

5 Member Governments and international organizations are invited to bring this circular to the attention of national Designated Authorities, Administrations, port facility security officer, maritime industry and all other parties concerned and responsible for the implementation of maritime security measures.

ANNEX

DRAFT MSC CIRCULAR
SHORE LEAVE AND ACCESS TO SHIPS UNDER THE ISPS CODE

1 The 2002 SOLAS Conference that adopted SOLAS chapter XI-2, the ISPS Code, and associated conference resolutions, was aware of potential human aspect problems affecting the fundamental human rights of seafarers with the imposition of a security regime on international shipping on a global basis. It was recognized that seafarers would have the primary duties and responsibilities for implementing the new security regime for ships. At the same time, there was concern that the emphasis on port facility security may result in the ship and seafarers being viewed as a potential threat to security rather than partners in the new security regime.

2 In this regard, it was recognized that there may be conflicts between security and human rights, as well as between security and the efficient movement of ships and cargoes in international trade that is essential to the global economy. There must be a proper balance between the needs of security, the protection of the human rights of seafarers and port workers, and the requirement to maintain the safety and working efficiency of the ship by allowing access to ship support services such as the taking on of stores, repair and maintenance of essential equipment, and other vital activities that are appropriately undertaken while moored at port facilities.

3 The 2002 SOLAS Conference incorporated the protection of the fundamental human rights of seafarers into SOLAS chapter XI-2 and the ISPS Code. The Preamble to the ISPS Code clearly states that the Code shall not be interpreted in a manner that is inconsistent with existing international instruments protecting the rights and freedoms of maritime and port workers. The Preamble also called to the attention of Contracting Governments that in approving security plans they should be aware of the need for seafarer's shore leave and access to shore-based welfare facilities and medical care.

4 To address these concerns and principles, section A/16.3.15 of the ISPS Code provides that a port facility security plan (PFSP) must contain procedures for facilitating shore leave, crew changes and access for visitors including representatives of seafarers' welfare and labour organizations. This should be construed as including shore-based ship support personnel and the taking onboard of ship's stores. The guidance contained in paragraph B/16.8.14 of the ISPS Code reinforces this requirement by providing that the PFSP should contain such procedures relating to all security levels.

5 In approving PFSPs, Contracting Governments must ensure that PFSPs address the procedures described in section A/16.3.15 of the ISPS Code, taking into account the guidance in paragraph B/16.8.14 of the ISPS Code.

6 From a practical perspective, it is also important that port facilities seek a balance between the needs of security and the needs of the ship and its crew. A port facility operator should ensure co-ordination of shore leave for ship personnel or crew change-out, as well as access through the port facility for visitors to the ship, including representatives of seafarers' welfare and labour organizations and those concerned with the maintenance of ships' equipment and safe operation, with ship operators in advance of the ship's arrival. A singular focus on the security of the port facility is contrary to the letter and spirit of the ISPS Code and will have

serious consequences for the international maritime transportation system that is a vital component of the global economy. It is further noted that the ILO/IMO Code of Practice for Port Security recommends that all port stakeholders work co-operatively to make such arrangements and advance plans.

7 As provided in Conference resolution 11 of the 2002 SOLAS Conference, Contracting Governments are urged to take the human element, the need to afford special protection to seafarers and the critical importance of shore leave into account when implementing the provisions of SOLAS chapter XI-2 and the ISPS Code. Therefore, Contracting Governments, Member States of the Organization, and non-governmental organizations with consultative status at Organization are encouraged to report to the Organization any instances where the human element has been adversely impacted by the implementation of the provisions of SOLAS chapter XI-2 and the ISPS Code and requests that they bring such instances to the attention of the Maritime Safety Committee and the Facilitation Committee.

_____